Informazioni sul flusso del traffico non HTTP del proxy gateway multicast

Sommario

Introduzione

Questo documento descrive come Cisco Multicast Defense Gateway gestisce il traffico TCP (diverso dal Web), quando viene configurato un proxy di inoltro.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del cloud computing
- Conoscenze base delle reti di computer

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Proxy

Un proxy funge da intermediario per due endpoint di rete. Funge da gateway per la transizione da una rete all'altra per applicazioni specifiche. I proxy controllano e semplificano la complessità delle richieste attraverso il processo di richiesta e le funzionalità di inoltro. Offrono diversi livelli di funzionalità, sicurezza e privacy e si rivelano utili per la navigazione sul Web e la protezione dei

dati.

.

Proxy di inoltro gateway multicast

Questo diagramma mostra il flusso di rete quando il gateway multicolore viene posizionato nel percorso tra il client e il server e il gateway multicolore è configurato per fungere da proxy di inoltro.

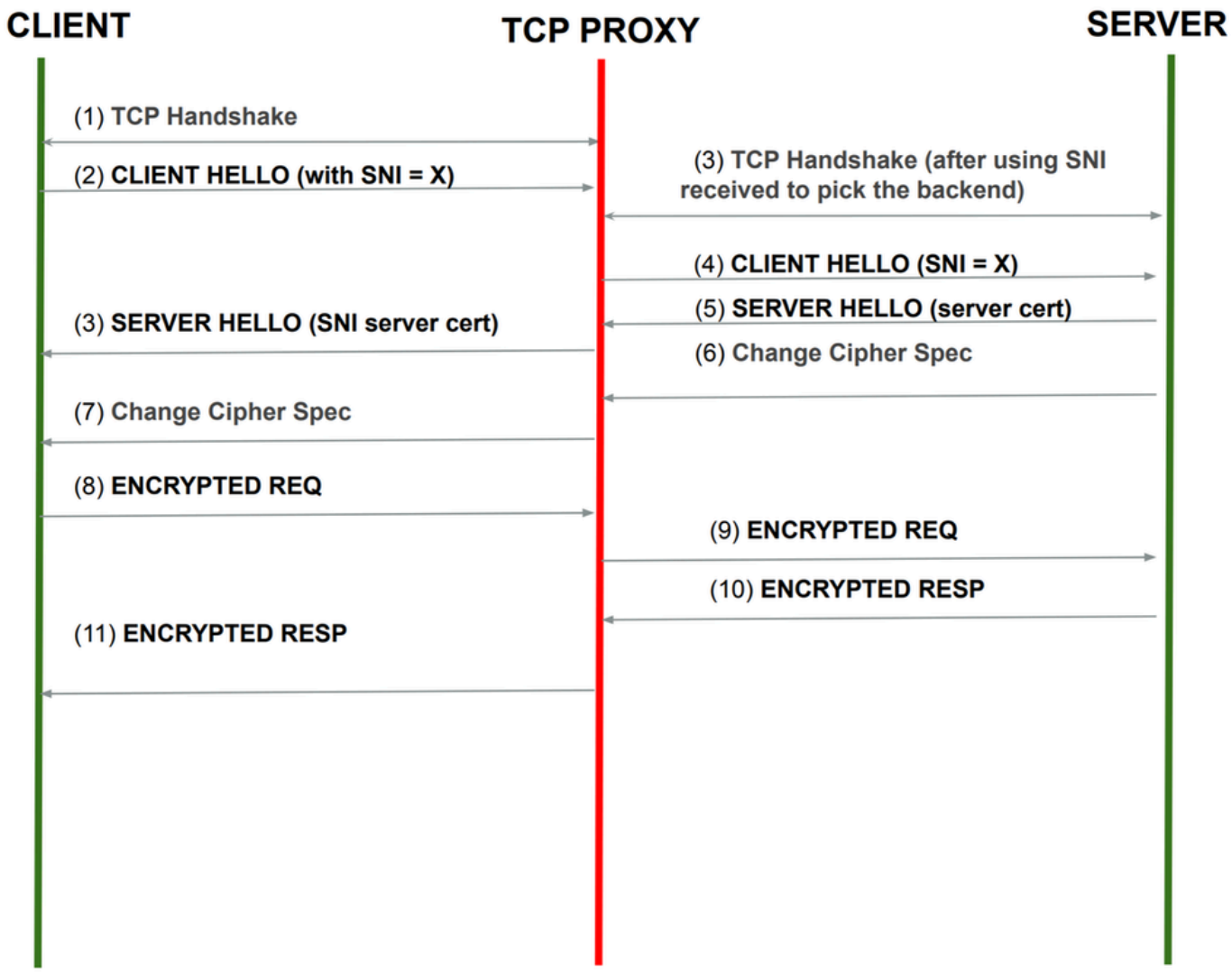
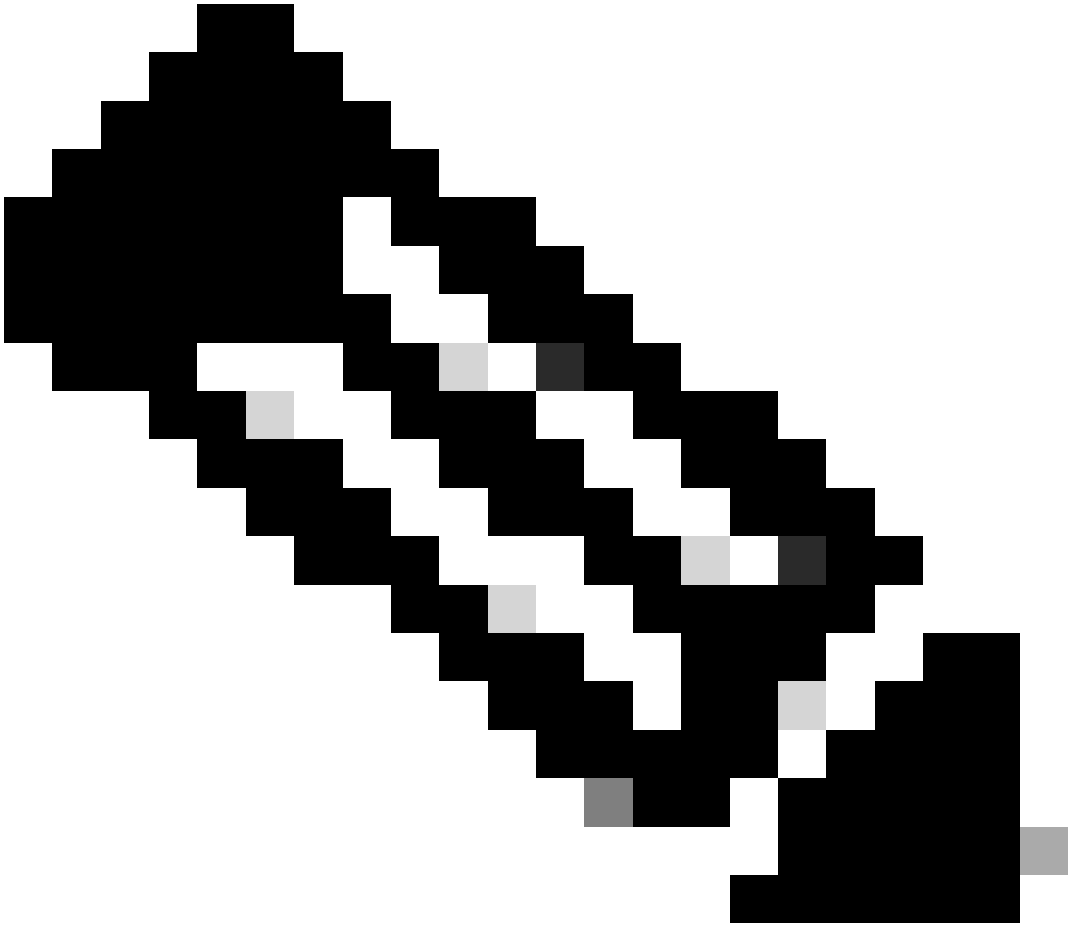
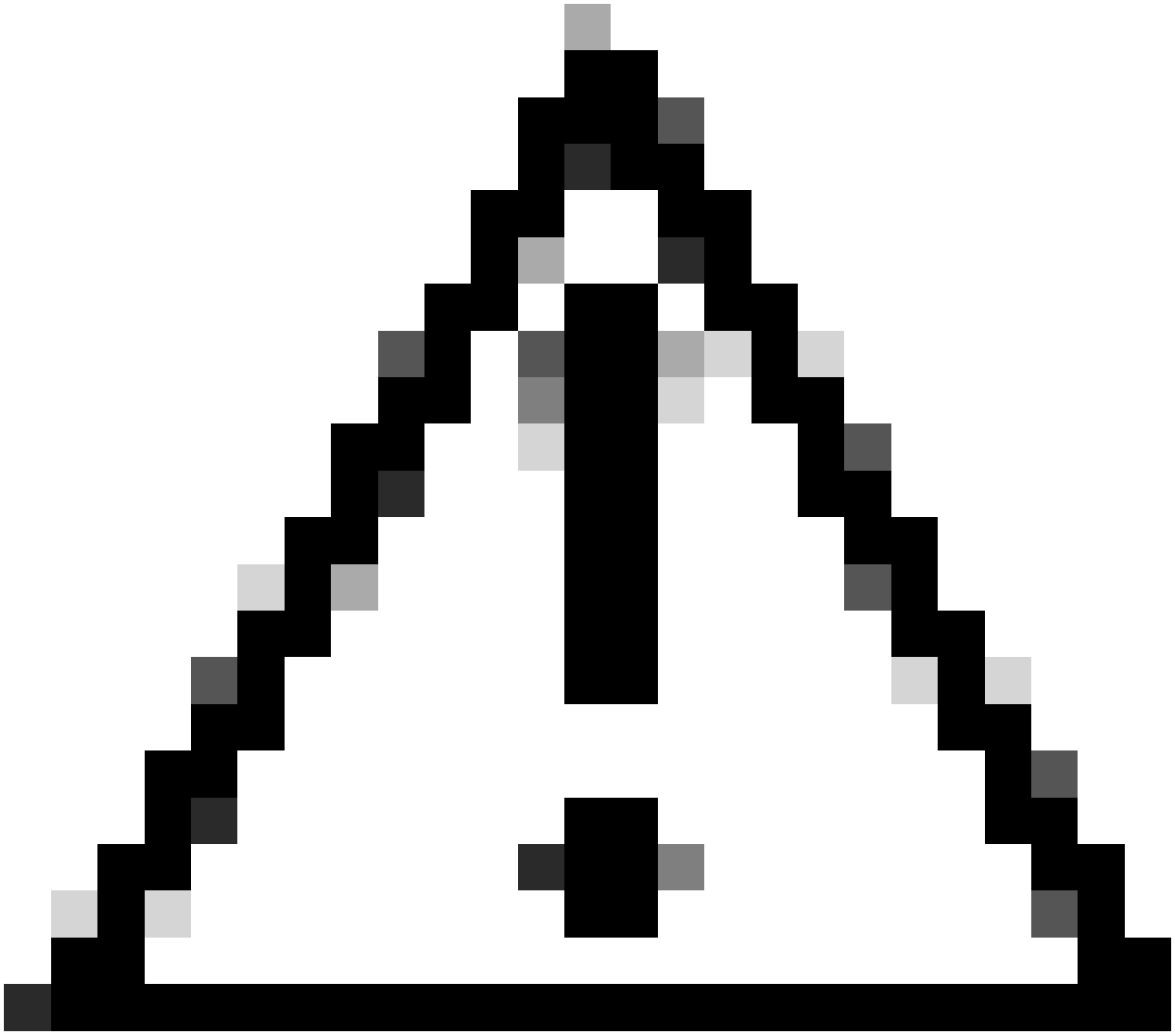


Immagine - MCD Forward Proxy



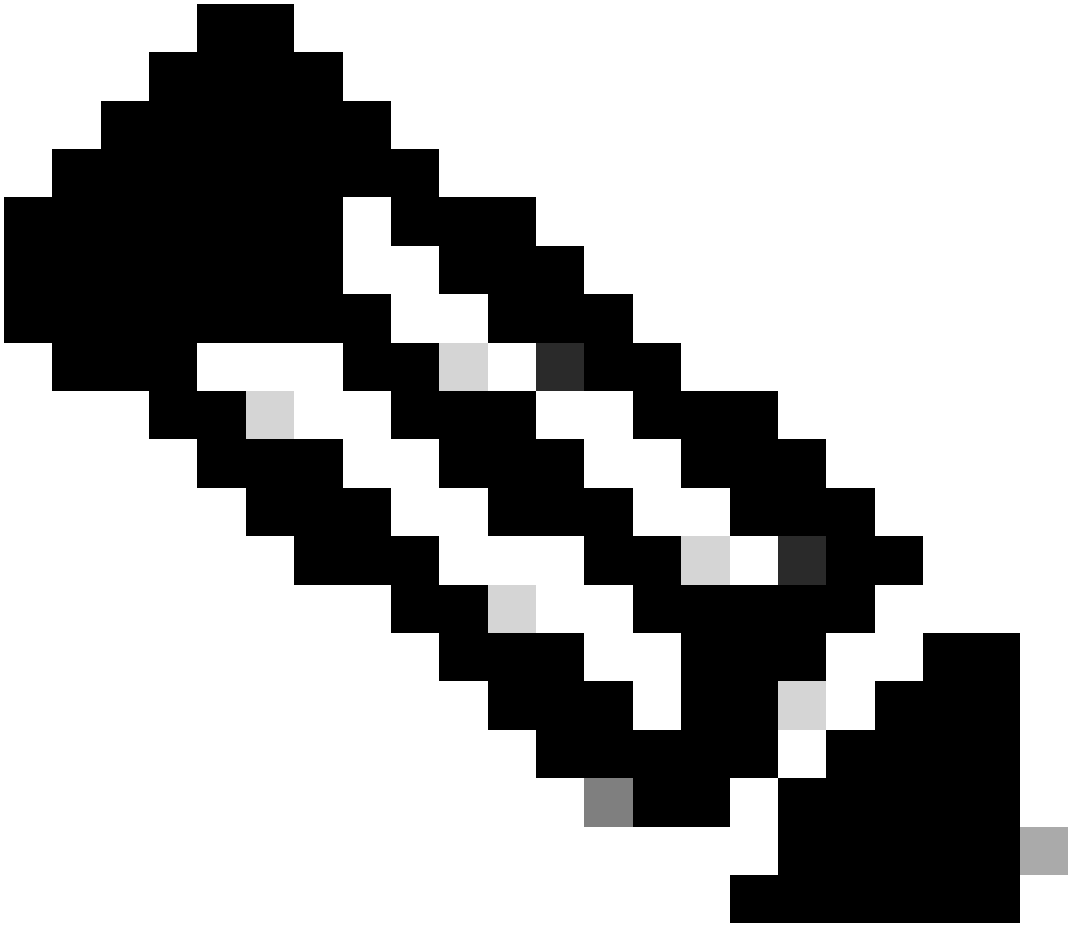
Nota: questo processo è applicabile al traffico SSH quando il client è configurato per utilizzare il gateway multicolore come proxy per la connessione al server SSH.

1. L'handshake a 3 vie TCP viene avviato tra il client e il gateway multicolore.
2. Il client invia un HELLO CLIENT al server. Questo HELLO CLIENT contiene l'identificatore del nome del server (SNI, Server Name Identifier). Il gateway intercetta questo pacchetto ed esegue i criteri di filtro FQDN.



Attenzione: alcune applicazioni configurate per utilizzare i protocolli di negoziazione automatica, ad esempio quelle che determinano la versione SSH, non devono trasmettere il messaggio Hello del client.

3. Se il traffico è consentito, il gateway avvia una nuova richiesta di handshake TCP al server e inoltra il client Hello. (ricevuto dal client)



Nota: se il server non ha ricevuto alcun pacchetto dal gateway a cloud multipli, è possibile che il client non abbia inviato il messaggio Hello.

4. Il gateway multicolore ha inoltrato il Server Hello al client.

5. Dopo lo scambio dei certificati, tutti i pacchetti vengono inviati così come sono senza alcuna azione

Informazioni correlate

- Guida per l'utente di Cisco Multicast Defense - Profilo filtro FQDN [Cisco Defense Orchestrator] - Cisco
- Domande frequenti - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).